

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Tadashi EZAKI

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: DELIVERY SYSTEM FOR DELIVERY ITEMS, DELIVERY AGENCY SERVER APPARATUS, CRYPTOGRAM READER, DELIVERY METHOD FOR DELIVERY ITEMS, PROGRAM, AND RECORDING MEDIUM

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed

☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

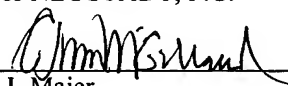
<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2002-272197	September 18, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
☐ are submitted herewith
☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.


Gregory J. Maier

Registration No. 25,599

C. Irvin McClelland
Registration Number 21,124

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 9月18日

出 願 番 号

Application Number:

特願2002-272197

[ST.10/C]:

[JP2002-272197]

出 願 人

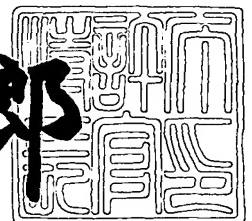
Applicant(s):

ソニー株式会社

2003年 6月19日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3048015

【書類名】 特許願

【整理番号】 0290109107

【提出日】 平成14年 9月18日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G06F 19/00

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 江崎 正

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

【代理人】

 【識別番号】 100095957

 【弁理士】

 【氏名又は名称】 亀谷 美明

 【電話番号】 03-5919-3808

【選任した代理人】

 【識別番号】 100096389

 【弁理士】

 【氏名又は名称】 金本 哲男

 【電話番号】 03-3226-6631

【選任した代理人】

 【識別番号】 100101557

 【弁理士】

 【氏名又は名称】 萩原 康司

 【電話番号】 03-3226-6631

【手数料の表示】

 【予納台帳番号】 040224

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0012374

【プルーフの要否】 要

配送業者サーバ装置、暗号読取装置、
本。

業者に委託する送付者の送付者端末装置
者端末装置とが、公衆回線網を介して接

アを介して前記配送業者の公開鍵を取得
配送物の配送に必要な受取者の個人情報
暗号情報を生成し、前記受取者暗号情報

た受取者暗号情報を前記配送業者に委託

記配送業者の暗号読取装置により、前記
暗号情報を復号化されて、前記受取人情

ム。

は、前記受取者暗号情報に前記配送業者
送付者端末装置に送信する、ことを特徴
システム。

は、所定のメディアを介して前記配送業
して、送付者に関する送付者情報を暗号
付者暗号情報を前記配送業者に委託する

記配送業者の暗号読取装置により、前記
暗号情報が復号化されて、前記送付者情

送物の配送システム。

者暗号情報は、コード化情報からなる、

ことを特徴とする請求項 1 に記載の配送物の配送システム。

【請求項 5】 少なくとも前記受取者暗号情報の出力には、少なくとも前記受取者を識別するための名称が記載されている、ことを特徴とする請求項 1 に記載の配送物の配送システム。

【請求項 6】 配送物の配送を配送業者に委託する送付者の送付者端末装置と、前記配送物を受け取る受取者の受取者端末装置と公衆回線網を介して接続される、前記送付者から委託された前記配送物を前記受取者に配送する配送業者の配送業者サーバ装置であって、

前記配送業者サーバ装置は、

少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報を暗号化する暗号化プログラムを実行させるための公開鍵を管理する公開鍵管理手段と

前記受取者端末装置の要求に応じて、前記公開鍵を前記受取者端末装置に送信する公開鍵送信手段と、

少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報が前記公開鍵を使用して前記暗号化プログラムにより暗号化されて生成された受取者暗号情報を、復号化するための秘密鍵を管理する秘密鍵管理手段と、

前記受取者暗号情報を復号化する暗号読取装置に対して、前記秘密鍵を提供する秘密鍵提供手段と、を有する、

ことを特徴とする配送業者サーバ装置。

【請求項 7】 さらに、

前記公開鍵送信手段は、前記送付者端末装置の要求に応じて、前記公開鍵を前記送付者端末装置に送信することが可能であり、

前記公開鍵を使用して、前記暗号化プログラムにより前記送付者に関する送付者情報を暗号化した送付者暗号情報の生成が可能であり、

前記秘密鍵は、前記送付者暗号情報を復号化することが可能である、

ことを特徴とする請求項 6 に記載の配送業者サーバ装置。

【請求項 8】 少なくとも前記受取者暗号情報の出力には、少なくとも前記受取者を識別するための名称が記載されている、ことを特徴とする請求項 6 に記

載の配送物の配送システム。

【請求項 9】 配送物の配送を配送業者に委託する送付者の送付者端末装置と、前記配送物を受け取る受取者の受取者端末装置と公衆回線網を介して接続される、前記送付者から委託された前記配送物を前記受取者に配送する配送業者の配送業者サーバ装置と接続可能な暗号読取装置であって、

前記配送業者の公開鍵を使用して暗号化プログラムにより少なくとも配送物の配送に必要な受取者情報が暗号化されて生成された受取者暗号情報を復号化するための秘密鍵をサーバ装置から取得する手段と、

前記受取者暗号情報を読み取って、前記秘密鍵により復号化する手段と、

前記復号化した受取者暗号情報を可読な受取者情報として出力する手段と、
を有することを特徴とする暗号読取装置。

【請求項 10】 前記暗号読取装置は、前記公開鍵を使用して前記暗号化プログラムにより暗号化された送付者の個人情報である送付者暗号情報の復号化が可能であり、

前記復号化した送付者暗号情報を可読な送付者情報として出力可能である、
ことを特徴とする請求項 9 に記載の暗号読取装置。

【請求項 11】 配送物の配送を配送業者に委託する送付者の送付者端末装置と、前記配送物を受け取る受取者の受取者端末装置とが、公衆回線網を介して接続された配送物の配送方法であって、

前記受取者端末装置は、所定のメディアを介して前記配送業者の公開鍵を取得し、前記公開鍵を使用して、少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報を暗号化して受取者暗号情報を生成し、前記受取者暗号情報を前記送付者端末装置に送信し、

前記送付者端末装置は、前記送信された受取者暗号情報を前記配送業者に委託する配送物に添付するために出力し、

前記出力された受取者暗号情報は、前記配送業者の暗号読取装置により、前記配送業者の秘密鍵を使用して前記受取者暗号情報を復号化されて、前記受取人の配達先の情報が前記配送業者に取得される、

ことを特徴とする配送物の配送方法。

【請求項 1 2】 前記受取者端末装置は、前記受取者暗号情報に前記配送業者の公開鍵に関する情報を添付して、前記送付者端末装置を送信する、ことを特徴とする請求項 1 1 に記載の配送物の配送方法。

【請求項 1 3】 前記送付者端末装置は、前記配送業者サーバ装置から又は所定のメディアを介して前記配送業者の公開鍵を取得し、前記公開鍵を使用して、送付者に関する情報を暗号化して送付者暗号情報を生成し、前記送付者暗号情報を前記配送業者に委託する配送物に添付するために出力し、

前記出力された送付者暗号情報は、前記配送業者の暗号読取装置により、前記配送業者の秘密鍵を使用して前記送付者暗号情報が復号化されて、前記送付者情報が前記配送業者に取得される、

ことを特徴とする請求項 1 1 に記載の配送物の配送方法。

【請求項 1 4】 少なくとも前記受取者暗号情報は、コード化情報からなることを特徴とする請求項 1 1 に記載の配送物の配送方法。

【請求項 1 5】 少なくとも前記受取者暗号情報の出力には、少なくとも前記受取者を識別するための名称が記載されている、ことを特徴とする請求項 1 1 に記載の配送物の配送方法。

【請求項 1 6】 配送物の配送を配送業者に委託する送付者の送付者端末装置と、前記配送物を受け取る受取者の受取者端末装置と公衆回線網を介して接続される、前記送付者から委託された前記配送物を前記受取者に配送する配送業者のコンピュータに対し、

少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報を暗号化する暗号化プログラムを実行させるための公開鍵を管理する公開鍵管理手段と、

前記受取者端末装置の要求に応じて、前記公開鍵を前記受取者端末装置に送信する公開鍵送信手段と、

少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報が前記公開鍵を使用して前記暗号化プログラムにより暗号化されて生成された受取者暗号情報を、復号化するための秘密鍵を管理する秘密鍵管理手段と、

前記受取者暗号情報を復号化する暗号読取装置に対して、前記秘密鍵を提供する秘密鍵提供手段と、
して機能させるためのプログラム。

【請求項 1 7】 配送物の配送を配送業者に委託する送付者の送付者端末装置と、前記配送物を受け取る受取者の受取者端末装置と公衆回線網を介して接続される、前記送付者から委託された前記配送物を前記受取者に配送する配送業者のコンピュータに対し、

少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報を暗号化する暗号化プログラムを実行させるための公開鍵を管理する公開鍵管理手段と、

前記受取者端末装置の要求に応じて、前記公開鍵を前記受取者端末装置に送信する公開鍵送信手段と、

少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報が前記公開鍵を使用して前記暗号化プログラムにより暗号化されて生成された受取者暗号情報を、復号化するための秘密鍵を管理する秘密鍵管理手段と、

前記受取者暗号情報を復号化する暗号読取装置に対して、前記秘密鍵を提供する秘密鍵提供手段と、

して機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、配送物の配送システム、配送業者サーバ装置、暗号読取装置、配送物の配送方法、プログラム、記録媒体に関し、さらに詳細には、受取者又は送付者の個人情報を相手方に開示することなく配送物を配送可能にする配送システムに関する。

【0 0 0 2】

【従来の技術】

近年においては、インターネットによるメール、掲示板、オークションなどを

介して物品が売買する方法が急速に利用されつつある。このようなインターネットを利用して物品を売買する方法では、物品の送付者及び受取人は共に、相手方に、自分の個人情報を知らせたくない場合が多い。また、インターネットショッピングを利用する場合にも、受取人の個人情報をショップ側に開示したくない場合がある。

【 0 0 0 3 】

このような問題を解決するために、個人情報を開示せずにインターネットショッピングを実行する方法として、配送サービス会社が I D 番号と個人情報を関連付けて格納するデータベースを有するサーバ装置を設置し、I D 番号だけをショップ側通知することにより、配送物を配送する方法が提案されている(例えば、特許文献 1 参照)

【 0 0 0 4 】

【特許文献 1】

特開 2 0 0 2 - 7 9 0 4 号公報

【 0 0 0 5 】

【発明が解決しようとする課題】

しかしながら、上記特許文献 1 にかかる方法では、サーバ装置のデータベースに格納されている情報の機密が十分に保持されるように管理しなければならない。したがって、サーバ装置の管理が不十分である場合には、個人情報が漏洩してしまうという問題がある。例えばデータベースごと盗難された場合には、データベースに登録されている個人情報が全て漏洩してしまうことになる。また、I D 番号を間違えて送信してしまうと、全く関係のない他人に配送物が配送されてしまう、という問題もある。さらに、配送業者は、必ずサーバ装置に問い合わせなければならないため、オフラインで使うことができない、という問題がある。

【 0 0 0 6 】

したがって、本発明の目的は、上記のように厳密な管理が必要な情報を格納するデータベースを設置することなく、送付者及び受取人の個人情報を秘密にした状態で配送物を配送することが可能な新規かつ改良された配送物の配送システム

等を提供することにある。

【 0 0 0 7 】

【課題を解決するための手段】

上記課題を解決するため、本発明の第 1 の観点においては、配送物の配送を配送業者に委託する送付者の送付者端末装置と、前記配送物を受け取る受取者の受取者端末装置とが、公衆回線網を介して接続されており、前記受取者端末装置は、所定のメディアを介して前記配送業者の公開鍵を取得し、前記公開鍵を使用して、少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報を暗号化して受取者暗号情報を生成し、前記受取者暗号情報を前記送付者端末装置に送信し、前記送付者端末装置は、前記送信された受取者暗号情報を前記配送業者に委託する配送物に添付するために出力し、前記出力された受取者暗号情報は、前記配送業者の暗号読取装置により、前記配送業者の秘密鍵を使用して前記受取者暗号情報を復号化されて、前記受取者情報が前記配送業者に取得される、ことを特徴とする配送物の配送システムが提供される。

【 0 0 0 8 】

上記記載の発明では、公開鍵を使用して、受取者の個人情報暗号化するので、個人情報を送付者に知られることなく配送物が配送される。このとき、受取者の個人情報あるいは送付者の個人情報を格納するためのデータベースが不要となるので、個人情報の流出が最大限防止することができる。例えば暗号キーが盗難された場合であっても、その暗号キーを使用した配送物に関する個人情報のみの漏洩に止めることができる。さらに、サーバ管理の手間がなくなるばかりでなく、個人情報を秘密にする配送システムを低コストで実現することができる。さらに、配送業者は、サーバ装置に問い合わせる必要がないので、オフラインで宛名を変換することができる。

【 0 0 0 9 】

また、前記受取者端末装置は、前記受取者暗号情報に前記配送業者の公開鍵に関する情報を添付して、前記送付者端末装置に送信する、如く構成すれば、その情報を参照することにより配送業者が複数の公開鍵・秘密鍵ペアを運用することができる。

【 0 0 1 0 】

また、前記送付者端末装置は、所定のメディアを介して公開鍵を取得し、前記公開鍵を使用して、送付者に関する送付者情報を暗号化して送付者暗号情報を生成し、前記送付者暗号情報を前記配送業者に委託する配送物に添付するため出力し、前記出力された送付者暗号情報は、前記配送業者の暗号読取装置により、前記配送業者の秘密鍵を使用して前記送付者暗号情報が復号化されて、前記送付者情報が前記配送業者に取得される、如く構成すれば、受取者には送付者の個人情報を知られることなく、配送業者は送付者の個人情報を認識することができる。

【 0 0 1 1 】

また、少なくとも前記受取者暗号情報は、コード化情報からなる、如く構成すれば、受取者暗号情報（必要に応じて送付者暗号情報）は、例えばバーコードまたは２次元バーコードなどのコード化情報からなるので、暗号読取装置により受取者情報（必要に応じて送付者情報）容易に自動認識することができる。

【 0 0 1 2 】

また、少なくとも前記受取者暗号情報の出力には、少なくとも、前記受取者を識別するための名称が記載されている、如く構成すれば、受取者の実名（必要に応じて送付者の実名）を明かすことなく、受取者（必要に応じて送付者）を識別することができる。

【 0 0 1 3 】

上記課題を解決するため、本発明の第２の観点においては、配送物の配送を配送業者に委託する送付者の送付者端末装置と、前記配送物を受け取る受取者の受取者端末装置と公衆回線網を介して接続される、前記送付者から委託された前記配送物を前記受取者に配送する配送業者の配送業者サーバ装置であって、前記配送業者サーバ装置は、少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報を暗号化する暗号化プログラムを実行させるための公開鍵を管理する公開鍵管理手段と、前記受取者端末装置の要求に応じて、前記公開鍵を前記受取者端末装置に送信する公開鍵送信手段と、少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報が前記公開鍵を使用して前記暗号化プログラ

ムにより暗号化されて生成された受取者暗号情報を、復号化するための秘密鍵を管理する秘密鍵管理手段と、前記受取者暗号情報を復号化する暗号読取装置に対して、前記秘密鍵を提供する秘密鍵提供手段と、を有する、ことを特徴とする配送業者サーバ装置が提供される。

【 0 0 1 4 】

上記記載の発明では、公開鍵を使用して、受取者の個人情報暗号化するので、個人情報を送付者に知られることなく配送物が配送するための配送業者サーバ装置が提供される。このとき、配送業者サーバ装置には、受取者の個人情報あるいは送付者の個人情報を格納するためのデータベースが不要となるので、個人情報の流出が最大限防止することができる。例えば暗号キーが盗難された場合であっても、その暗号キーを使用した配送物に関する個人情報のみの漏洩に止めることができる。さらに、サーバ管理の手間がなくなるばかりでなく、個人情報を秘密にする配送システムを低コストで実現することができる。さらに、配送業者は、サーバ装置に問い合わせる必要がないので、オフラインで宛名を変換することができる。

【 0 0 1 5 】

また、さらに、前記公開鍵送信手段は、前記送付者端末装置の要求に応じて、前記公開鍵を前記送付者端末装置に送信することが可能であり、前記公開鍵を使用して、前記暗号化プログラムにより前記送付者に関する送付者情報を暗号化した送付者暗号情報の生成が可能であり、前記秘密鍵は、前記送付者暗号情報を復号化することが可能である、如く構成すれば、受取者には送付者の個人情報が知られることなく、配送業者は送付者の個人情報を認識することができる。

【 0 0 1 6 】

また、少なくとも前記受取者暗号情報の出力には、少なくとも、前記受取者を識別するための名称が記載されている、如く構成すれば、受取者の実名（必要に応じて送付者の実名）を明かすことなく、受取者（必要に応じて送付者）を識別することができる。

【 0 0 1 7 】

上記課題を解決するため、本発明の第3の観点においては、配送物の配送を配

送業者に委託する送付者の送付者端末装置と、前記配送物を受け取る受取者の受取者端末装置と公衆回線網を介して接続される、前記送付者から委託された前記配送物を前記受取者に配送する配送業者の配送業者サーバ装置と接続可能な暗号読取装置であって、前記配送業者の公開鍵を使用して暗号化プログラムにより少なくとも配送物の配送に必要な受取者情報が暗号化されて生成された受取者暗号情報を復号化するための秘密鍵をサーバ装置から取得する手段と、前記受取者暗号情報を読み取って、前記秘密鍵により復号化する手段と、前記復号化した受取者暗号情報を可読な受取者情報として出力する手段と、を有することを特徴とする暗号読取装置が提供される。

【 0 0 1 8 】

上記記載の発明では、配送業者は、暗号化された受取者の個人情報を送付者に知られることなく容易に解読することができる。また、サーバ装置に問い合わせる必要がないので、オフラインで宛名を変換することができる。

【 0 0 1 9 】

前記暗号読取装置は、前記公開鍵を使用して前記暗号化プログラムにより暗号化された送付者の個人情報である送付者暗号情報の復号化が可能であり、前記復号化した送付者暗号情報を可読な送付者情報として出力可能である、如く構成すれば、配送業者は、暗号化された送付者の個人情報を受取者に知られることなく容易に解読することができる。

【 0 0 2 0 】

上記課題を解決するため、本発明の第4の観点においては、配送物の配送を配送業者に委託する送付者の送付者端末装置と、前記配送物を受け取る受取者の受取者端末装置とが、公衆回線網を介して接続された配送物の配送方法であって、前記受取者端末装置は、所定のメディアを介して前記配送業者の公開鍵を取得し、前記公開鍵を使用して、少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報を暗号化して受取者暗号情報を生成し、前記受取者暗号情報を前記送付者端末装置に送信し、前記送付者端末装置は、前記送信された受取者暗号情報を前記配送業者に委託する配送物に添付するために出力し、前記出力された受取者暗号情報は、前記配送業者の暗号読取装置により、前記配送業者の秘密

鍵を使用して前記受取者暗号情報を復号化されて、前記受取人の配達先の情報が前記配送業者に取得される、ことを特徴とする配送物の配送方法が提供される。

【 0 0 2 1 】

上記記載の発明では、公開鍵を使用して、受取者の個人情報暗号化するので、個人情報を送付者に知られることなく配送物が配送される。このとき、受取者の個人情報あるいは送付者の個人情報を格納するためのデータベースが不要となるので、個人情報の流出が最大限防止することができる。例えば暗号キーが盗難された場合であっても、その暗号キーを使用した配送物に関する個人情報のみの漏洩に止めることができる。さらに、サーバ管理の手間がなくなるばかりでなく、個人情報を秘密にする配送システムを低コストで実現することができる。さらに、配送業者は、サーバ装置に問い合わせる必要がないので、オフラインで宛名を変換することができる。

【 0 0 2 2 】

また、前記受取者端末装置は、前記受取者暗号情報に前記配送業者の公開鍵に関する情報を添付して、前記送付者端末装置を送信する、如く構成すれば、その情報を参照することにより配送業者が複数の公開鍵・秘密鍵ペアを運用することができる。

【 0 0 2 3 】

また、前記送付者端末装置は、前記配送業者サーバ装置から又は所定のメディアを介して前記配送業者の公開鍵を取得し、前記公開鍵を使用して、送付者に関する情報を暗号化して送付者暗号情報を生成し、前記送付者暗号情報を前記配送業者に委託する配送物に添付するために出力し、前記出力された送付者暗号情報は、前記配送業者の暗号読取装置により、前記配送業者の秘密鍵を使用して前記送付者暗号情報が復号化されて、前記送付者情報が前記配送業者に取得される、如く構成すれば、受取者には送付者の個人情報が知られることなく、配送業者は送付者の個人情報を認識することができる。

【 0 0 2 4 】

また、少なくとも前記受取者暗号情報は、コード化情報からなる、如く構成すれば、受取者暗号情報（必要に応じて送付者暗号情報）は、例えばバーコードま

たは2次元バーコードなどのコード化情報からなるので、暗号読取装置により受取者情報（必要に応じて送付者情報）容易に自動認識することができる。

【 0 0 2 5 】

また、少なくとも前記受取者暗号情報の出力には、少なくとも、前記受取者を識別するための名称が記載されている、如く構成すれば、受取者の実名（必要に応じて送付者の実名）を明かすことなく、受取者（必要に応じて送付者）を識別することができる。

【 0 0 2 6 】

上記課題を解決するため、本発明の第5の観点においては、配送物の配送を配送業者に委託する送付者の送付者端末装置と、前記配送物を受け取る受取者の受取者端末装置と公衆回線網を介して接続される、前記送付者から委託された前記配送物を前記受取者に配送する配送業者のコンピュータに対し、少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報を暗号化する暗号化プログラムを実行させるための公開鍵を管理する公開鍵管理手段と、前記受取者端末装置の要求に応じて、前記公開鍵を前記受取者端末装置に送信する公開鍵送信手段と、少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報が前記公開鍵を使用して前記暗号化プログラムにより暗号化されて生成された受取者暗号情報を、復号化するための秘密鍵を管理する秘密鍵管理手段と、前記受取者暗号情報を復号化する暗号読取装置に対して、前記秘密鍵を提供する秘密鍵提供手段と、して機能させるためのプログラムが提供される。

【 0 0 2 7 】

上記課題を解決するため、本発明の第6の観点においては、配送物の配送を配送業者に委託する送付者の送付者端末装置と、前記配送物を受け取る受取者の受取者端末装置と公衆回線網を介して接続される、前記送付者から委託された前記配送物を前記受取者に配送する配送業者のコンピュータに対し、少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報を暗号化する暗号化プログラムを実行させるための公開鍵を管理する公開鍵管理手段と、前記受取者端末装置の要求に応じて、前記公開鍵を前記受取者端末装置に送信する公開鍵送信手段と、少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報が

前記公開鍵を使用して前記暗号化プログラムにより暗号化されて生成された受取者暗号情報を、復号化するための秘密鍵を管理する秘密鍵管理手段と、前記受取者暗号情報を復号化する暗号読取装置に対して、前記秘密鍵を提供する秘密鍵提供手段と、して機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体が提供される。

【 0 0 2 8 】

【発明の実施の形態】

以下に添付図面を参照しながら、本発明の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。

【 0 0 2 9 】

(第 1 の実施の形態)

まず、図 1 に基づいて、本実施形態にかかる配送物の配送システムについて説明する。なお、図 1 は、本実施形態にかかる配送物の配送システムの構成を示すブロック図である。

【 0 0 3 0 】

まず、図 1 に示すように、本実施形態にかかる配送物の配送システム 1 0 は、受取者端末装置 1 0 0、送付者端末装置 2 0 0、配送業者サーバ装置 3 0 0 などがインターネット等を介して接続されている。なお、本実施形態にかかる配送業者サーバ装置 3 0 0 は、配送物の配送サービスを提供する事業者のサーバ装置であり、配送業者の暗号読取装置 4 0 0 とデータ転送可能に接続することができる。なお、受取者端末装置 1 0 0 及び送付者端末装置 2 0 0 は、プロバイタ 6 0 0、6 2 0 及び通信キャリア 7 0 0、7 2 0 を介して接続される。

【 0 0 3 1 】

また、ドメインネームサーバ 8 0 0 は、ドメイン名と I P アドレスの相互変換を実行し、受取者端末装置 1 0 0 あるいは送付者端末装置 2 0 0 から送信された URL 等から I P アドレスを検索して受取者端末装置 1 0 0 あるいは送付者端末装置 2 0 0 に返送する。

【 0 0 3 2 】

プロバイダ 6 0 0, 6 2 0 は, 通信キャリア 7 0 0, 7 2 0 を介して接続された受取者端末装置 1 0 0 とネットワーク 5 0 0 とを論理的に接続し, 受取者端末装置 1 0 0 とネットワーク 5 0 0, 及び送付者端末装置 2 0 0 とネットワーク 5 0 0 との間で情報伝達を可能とする。かかる通信キャリア 7 0 0, 7 2 0 は, 例えば N T T などの通信サービス会社が提供する伝送媒体が該当し, 受取者端末装置 1 0 0 とプロバイダ 6 0 0, 及び送付者端末装置 2 0 0 とプロバイダ 6 2 0 との間の接続及び情報の伝達を可能としている。

【 0 0 3 3 】

受取者端末装置 1 0 0 は, 図 2 に示すように, 配送業者サーバ装置 3 0 0 との通信を制御する通信制御装置 2 1 0, 配送業者サーバ装置 3 0 0 から送信されたコンテンツを表示する表示手段 (ディスプレイ) 1 2 0, 情報データなどの各種データを入力するための入力手段 1 3 0, 配送業者サーバ装置 3 0 0 から送信された情報を記憶するための記憶手段 1 4 0, などから構成される。なお, 記憶手段 1 4 0 には, 配送業者サーバ装置 3 0 0 から送信された暗号化プログラム, 公開鍵なども格納することができる。なお, 受取者端末装置 1 0 0 は, デスクトップコンピュータ, ノート型パーソナルコンピュータ, 携帯型端末以外にも, i モード (商標名) などのブラウザ機能を有する携帯電話及びパーム等通信機能を有する端末も含まれる。

【 0 0 3 4 】

かかる受取者端末装置 1 0 0 は, 少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報を, 配送業者の公開鍵を使用して, 予めダウンロードした配送業者の暗号化プログラムにより暗号化して, 受取者暗号情報として送付者端末装置 2 0 0 に送信する。

【 0 0 3 5 】

送付者端末装置 2 0 0 は, 図 3 に示すように, 配送業者サーバ装置 3 0 0 との通信を制御する通信制御装置 2 1 0, 配送業者サーバ装置 3 0 0 から送信されたコンテンツを表示する表示手段 (ディスプレイ) 2 2 0, 情報データなどの各種データを入力するための入力手段 2 3 0, 配送業者サーバ装置 3 0 0 から送信された情報を記憶するための記憶手段 2 4 0, 受取者暗号情報を例えばラベル印刷

により出力する出力手段 2 5 0 などから構成される。

【 0 0 3 6 】

記憶手段 2 4 0 には、配送業者サーバ装置 3 0 0 から送信された暗号化プログラム、公開鍵なども格納することができる。また、出力手段 2 5 0 は、受取者暗号情報をラベル印刷する以外にも、磁気カード、I C カードなどの各種媒体に記録するように出力することも含まれる。また、送付者端末装置 2 0 0 は、デスクトップコンピュータ、ノート型パーソナルコンピュータ、携帯型端末以外にも、i モード（商標名）などのブラウザ機能を有する携帯電話及びパーム等の通信機能を有する端末も含まれる。

【 0 0 3 7 】

次いで、図 4 に基づいて、本実施形態にかかる配送業者サーバ装置について説明する。なお、図 4 は、本実施形態にかかる配送業者サーバ装置の構成を示すブロック図である。なお、本実施形態にかかる配送業者サーバ装置は、従来と異なり、受取者の個人情報あるいは送付者の個人情報を格納するためのデータベースは設置されていない。

【 0 0 3 8 】

本実施形態にかかる配送業者サーバ装置 3 0 0 は、図 4 に示すように、CPU 3 1 0、通信ユニット 3 2 0、メモリ 3 3 0、暗号プログラム管理手段 3 4 0、公開鍵管理手段 3 5 0、秘密鍵管理手段 3 6 0、コンテンツデータベース 3 7 0 などから構成される。

【 0 0 3 9 】

CPU 3 1 0 は、配送業者サーバ装置 3 0 0 の全体制御を実行する。通信ユニット 3 2 0 は、電話回線を介した外部との通信や、例えばインターネットを介した外部との通信を制御するユニットである。メモリ 3 3 0 は、CPU 3 1 0 によって、アクセスされるためのプログラムやデータが格納される。

【 0 0 4 0 】

暗号化プログラム管理装置 3 4 0 には、受取者情報あるいは送付者情報を暗号化するためのプログラムが格納されている。公開鍵管理装置 3 5 0 は、暗号化プログラムを実行するための公開鍵が管理されている。秘密鍵管理手段 3 6 0 は、

暗号化された受取者情報あるいは送付者情報を復号化するための秘密鍵が管理されている。

【 0 0 4 1 】

コンテンツデータベース 3 7 0 には、配送業者サーバ装置 3 0 0 が提供する HTML ファイル、グラフィカル・アイコン・ファイル（G I F ファイルなど）、音声、画像オブジェクトなどのハイパーテキストオブジェクトなどのコンテンツが格納され、例えばインターネットを介して、これらのオブジェクトが受取者端末装置 1 0 0 及び送付者端末装置 2 0 0 に提供される。

【 0 0 4 2 】

暗号読取装置 4 0 0 は、受取者暗号情報を読み取るスキニング機能と、ダウンロードした秘密鍵を格納する秘密鍵格納機能と、読み取った受取者暗号情報を復号化する復号化機能と、復号化した受取者情報を例えばラベル印刷するラベル印刷機能などを有する。例えば、ラベル印刷機能付きハンディバーコードスキャナなどが含まれる。また、暗号読取装置 4 0 0 は、配送業者サーバ装置 3 0 0 と接続して、秘密鍵をダウンロードすることができる。

【 0 0 4 3 】

次に、図 5 を参照しながら図 6 に基づいて、本実施形態にかかる配送物の配送方法について説明する。なお、図 5 は、本実施形態にかかる配送物の配送方法を示す概念図である。図 6 は、本実施形態にかかる配送物の配送方法を示すフローチャートである。

【 0 0 4 4 】

本実施形態においては、まず、ユーザ同士がインターネットを利用して、例えば物品の売買が成立したことなどにより、配送物を配送する場合について説明する。このとき、受取者は、配送業者により配送された物品を受領する者である。送付者は、物品を所有、販売、貸与等する者あるいは業者であって、受取者に物品を送付する者である。また、受取者端末装置には、既に暗号化プログラムがダウンロードされているものとして説明する。

【 0 0 4 5 】

まず、図 6 に示すように、ステップ S 1 0 0 で、受取者端末装置 1 0 0 は、配

送業者Cの公開鍵K_pを取得する（ステップS100）。

【0046】

次いで、ステップS102で、受取者端末装置100は、取得した公開鍵K_pを使用して、予めダウンロードされている暗号化プログラムにより配送物の配送先である受取者の配送情報（例えば住所、氏名、電話番号などの受取者情報）を暗号化（例えばバーコード化）して、メール等などの電子的手段により送付者端末装置300に送信する（ステップS102）。

【0047】

その後、ステップS104で、送付者端末装置200は、受取者暗号情報を例えばラベルにプリントアウトし、暗号化された受取者情報が記載されたラベルを配送物に添付して配送業者Cに渡して配送を委託する（ステップS104）。

【0048】

さらに、ステップ106で、配送業者Cは、暗号読取装置（例えばバーコード読取用スキャナ）400により、配達業者Cの秘密鍵K_sを使用して受取者配送情報を復号化し、受取者Bの配達先が可読に明示されたラベルを印刷する（ステップS106）。なお、受領者Bの配達先が可読に明示されたラベルは、これまで貼り付けられていた暗号化されている表示ラベルと張り替えられる。

【0049】

最後に、ステップS106で、配送業者Cは、ラベルに明示された受取者Bの住所に配送物を配送し、受取者Bは、配送物を受け取ることができる（ステップS106）。

【0050】

本実施形態においては、受取者Bの配送情報（例えば、住所、氏名、電話番号などの受取者情報）が暗号化されて送付者Aに送信されるので、秘密鍵を有しない送付者Aに対して受取者情報が秘密にされる。このように、受取者Bの個人情報は、送付者Aに開示されることなく、配送物が受取者Bに配送される。

【0051】

また、上記配送物の配送システムにおいては、受取者情報のみを暗号化する例を挙げて説明したが、送付者Aの個人情報を暗号化することもできる。即ち、送

付者の身元情報（例えば住所、氏名など）についても、配送履歴を管理するなどの理由により、配送業者が知っておく必要もある。この場合において、送付者 A の個人情報（住所、氏名など）を配送物に添付してしまうと、送付者 A の個人情報が受取者に開示されてしまう。このため、送付者 A は、送付者端末装置 2 0 0 により上記受取者情報を暗号化すると同様の方法で送付者 A の個人情報を暗号化し、送付者 A の個人情報を受取者 B に開示することなく配送業者 C にのみ知らせることもできる。

【 0 0 5 2 】

以下、図 7 に基づいて、簡単に説明する。なお、受取者端末装置 1 0 0 から受取者暗号情報が送付者端末装置 2 0 0 に送信されている点は、図 5 と同様である。

【 0 0 5 3 】

図 7 に示すように、送付者端末装置 2 0 0 は、送付者 A の身元情報（例えば住所、氏名などの送付者情報）を配送業者 C の公開鍵 K_p を使用して暗号化プログラムにより暗号化して送付者暗号情報を生成し、受取人暗号情報と共に例えばラベルに印刷する。次いで、送付者暗号情報及び受取者暗号情報が印刷されたラベルを配送物に配送業者 C に引き渡す。

【 0 0 5 4 】

このことにより、配送業者 C は、配送業者 C の秘密鍵 K_s により送付者 A の個人情報を取得することができるが、秘密鍵 K_s を有しない受取者 B には、送付者 A の個人情報が開示されることはない。

【 0 0 5 5 】

次に、本実施形態にかかる配送物の配送方法の各工程について、図 8 ～図 2 1 に基づいて詳細に説明する。なお、本実施形態においては、①. 受取者情報の暗号化方法、②. 受取者暗号情報（及び送付者暗号情報）のラベル印刷、③. 受取者暗号情報の復号化の 3 つの工程に分けて説明する。

【 0 0 5 6 】

(1) 受取者情報の暗号化方法

以下に、本実施形態にかかる受取者情報の暗号化方法を図 8 ～図 1 7 に基づい

て詳細に説明する。

【 0 0 5 7 】

まず、受取者の暗号化の方法としては、例えば2種類の方法が考えられる。第1の暗号化方法は、受取者端末装置に格納された暗号化プログラムを使用して受取者情報を暗号化する方法である。第2の暗号化方法は、配送業者サーバ装置に格納されている暗号化プログラムを使用して受取者情報を暗号化する方法である。

【 0 0 5 8 】

(第1の暗号化方法：暗号化プログラムが受取者端末装置に格納されている場合の暗号化方法)

まず、本実施形態にかかる受取者の配送情報の第1の暗号化方法を図8～図13に基づいて、説明する。なお、図8は、本実施形態にかかる受取者情報の第1の暗号化方法を示す概念図である。図9は、本実施形態にかかる受取者情報の第1の暗号化方法を説明するためのフローチャートである。

【 0 0 5 9 】

まず、図9に示すように、ステップS200で、受取者端末装置100は、インターネットの配送業者Cのサイトから暗号化ソフトのプログラムをダウンロードして、インストールする(ステップS200)。なお、かかる暗号化プログラムは、例えば雑誌等の付録(例えばCD-ROM)として配布することもできる。

【 0 0 6 0 】

次いで、ステップS202では、図8に示すように、受取者端末装置100は、配送業者Cの公開鍵K_pをダウンロードして入手する(ステップS202)。なお、公開鍵は、本実施形態にかかる受取者情報の暗号化プログラムを実行するために必要な鍵である。

【 0 0 6 1 】

その後、ステップS204で、暗号化ソフトを立ち上げると、受取者端末装置100には、受取者Bの情報の入力画面が表示される(ステップS204)。なお、受取者情報入力画面は、図10に示すように、例えば、「ハンドルネーム

」，「住所」，「氏名」，「電話番号」などの入力項目と，「確認ボタン」が表示される。

【 0 0 6 2 】

さらに，ステップ S 2 0 6 で，受取者 B の配送情報の入力画面の各項目を入力する（ステップ S 2 0 6）。なお，「ハンドルネーム」は，受取者を識別するための名称を自由に記載する。「住所」は，受取者の住所であって，配送物を受け取る場所を記載する。「氏名」は，受取者本人の氏名を記載する。「電話番号」は，受取者の電話番号を記載する。「確認ボタン」は，受取者情報を暗号化する前に再確認するためのボタンである。

【 0 0 6 3 】

さらに，所定項目の入力が終了した後，確認ボタンをクリックすると，図 1 1 に示すように，受取者情報の確認画面が表示される。なお，「暗号化（OK）ボタン」は，受取者情報を暗号化を開始するためのボタンである。

【 0 0 6 4 】

さらに，ステップ S 2 0 8 で，受取者情報確認画面の暗号化ボタンをクリックすることにより，受取者情報の暗号化が実行される（ステップ S 2 0 8）。なお，受取者情報の暗号化は，例えば 1 6 進テキストコードにより暗号化することができるが，配送の手間を考慮して，例えばバーコードや 2 次元バーコードなどのコード化情報とするのが好ましい。かかるバーコードなどのコード化情報によれば，暗号読取装置により受取者暗号情報を容易に自動認識することができる。

【 0 0 6 5 】

最後に，ステップ S 2 1 0 で，受取者端末装置 1 0 0 により指定されディレクトリに受取者暗号情報のファイルが生成される（ステップ S 2 1 0）。かかるディレクトリの指定は，図 1 2 に示すように，ディレクトリ指定画面上で暗号化ファイルを保存するディレクトリを指定し，「OKボタン」をクリックすることにより実行することができる。なお，暗号化情報のファイル形式は，そのままラベルにできる画像ファイルフォーマット（G I F，J P E G，B M P など）としても良く，あるいは W O R D や P D F などのドキュメントファイルとしても良い。また，後続の処理ある送付者暗号情報（コード情報）と連結して出力することを

考慮すれば、単なるバイナリーのデータとするのが好ましい。

【 0 0 6 6 】

なお、生成されたファイルには、受取者暗号情報と共に、受取者を識別するための名称（例えばハンドルネーム）や、知られても構わないメールアドレスなどが記載されているのが好ましい。

【 0 0 6 7 】

このようにして、受取者端末装置に格納されている暗号化プログラムを利用して、受取者情報は暗号化されて、受取者 B が指定したディレクトリに保存することができる。

【 0 0 6 8 】

（第 2 の暗号化方法：暗号化プログラムが配送業者サーバ装置に格納されている場合の暗号化方法）

次に、本実施形態にかかる受取者の配送情報の第 2 の暗号化方法を図 1 3 ～ 図 1 7 に基づいて、説明する。なお、図 1 3 は、本実施形態にかかる受取者情報の第 2 の暗号化方法を示す概念図である。図 1 4 は、本実施形態にかかる受取者情報の第 2 の暗号化方法を説明するためのフローチャートである。

【 0 0 6 9 】

まず、ステップ S 3 0 0 で、受取者端末装置 1 0 0 は、通常のインターネットブラウザで配送業者 C の W e b サイトにアクセスする（ステップ S 3 0 0）。

【 0 0 7 0 】

次いで、ステップ S 3 0 2 で、本実施形態にかかる配送物の配送システムを使用するための S S L 使用可能なページ（受取者情報入力ページ）に移行し、S S L 起動ボタン（図示せず）をクリックして S S L を起動する（ステップ S 3 0 2）。このことにより、暗号化通信可能な状態で、本実施形態にかかる配送物の配送システムを使用することができる。なお、受取者情報入力画面は、図 1 5 に示すように、例えば、「ハンドルネーム」、「住所」、「氏名」、「電話番号」などの入力項目と、「確認ボタン」が表示される。

【 0 0 7 1 】

その後、ステップ S 3 0 4 で、画面上に表示された受取者情報の入力画面に所

定項目を入力する（ステップ S 3 0 4）。なお、「ハンドルネーム」は、受取者を識別するための名称を自由に記載する。「住所」は、受取者の住所であって、配送物を受け取る場所を記載する。「氏名」は、受取者本人の氏名を記載する。

「電話番号」は、受取者の電話番号を記載する。「確認ボタン」は、受取者情報を暗号化する前に再確認するためのボタンである。

【 0 0 7 2 】

さらに、所定項目の入力が終了した後、「確認ボタン」をクリックすると、図 1 6 に示すように、受取者情報の確認画面が表示される。なお、「暗号化（OK）ボタン」は、受取者情報を暗号化を開始するためのボタンである。

【 0 0 7 3 】

さらに、ステップ S 3 0 6 で、受取者情報確認画面の「暗号化ボタン」をクリックすることにより、図 1 3 に示すように、配送業者サーバ装置に受取者情報が転送されて暗号化が実行される（ステップ S 3 0 6）。なお、受取者情報の暗号化は、例えば 1 6 進テキストコードにより暗号化することもできるが、配送の手間を考慮して、例えばバーコードや 2 次元バーコードなどのコード化情報とするのが好ましい。かかるバーコードなどのコード化情報によれば、暗号読取装置で受取者暗号情報を容易に自動認識することができる。

【 0 0 7 4 】

その後、ステップ S 3 0 8 で、図 1 3 に示すように、受取者端末装置 1 0 0 により指定されたメールアドレスにファイルが送信される（ステップ S 3 0 8）。かかるメールアドレスの指定は、図 1 7 に示すように、メールアドレス指定画面上で暗号化ファイルを送信するメールアドレスを指定することができる。そして、「OKボタン」をクリックすることにより、暗号化ファイルの送信が実行される。なお、暗号化情報のファイル形式は、そのままラベルにできる画像ファイルフォーマット（G I F, J P E G, B M P など）としても良く、あるいは W O R D や P D F などのドキュメントファイルとしても良い。また、後続の処理ある送付者暗号情報（コード情報）と連結して出力することを考慮すれば、単なるバイナリーのデータとするのが好ましい。

【 0 0 7 5 】

このようにして、配送業者サーバ装置に格納されている暗号化プログラムを利用して、受取者情報は暗号化されて、受取者Bが指定したメールアドレスに送信される。なお、暗号化ファイルはサイト上に置き、受取者端末装置が例えばf t pまたはh t t pによりダウンロードすることにより受取者端末装置は暗号化情報を取得することもできる。

【 0 0 7 6 】

(2) 受取者暗号情報（及び送付者暗号情報）のラベル印刷

上記のように暗号化された受取者情報は、受取者端末装置から送付者端末装置に送信されて、ラベル印刷される。

【 0 0 7 7 】

かかるラベルの例を図18、図19に基づいて説明する。なお、図18は、受取者暗号情報をラベルに表示した一例を示す。図19は、受取者暗号情報及び送付者暗号情報をラベルに表示した一例を示す。

【 0 0 7 8 】

まず、図18に示すように、受取者暗号情報を表示した配送ラベルには、「配送先」、「宛先」が表示されている。「配送先」は、配送業者の住所、会社名、営業所名が記載されている。「宛先」は、受取者を識別するための名称であるハンドルネーム（HN）、暗号化された受取者情報、メールアドレスが記載されている。このように、ラベルには、受取者の宛先に関する情報は暗号化されて表示され、受取者の個人情報は一切表示されることはない。

【 0 0 7 9 】

また、送付者暗号情報を受取者暗号情報を併記してラベル表示することもできる。かかる場合は、図19に示すように、ラベルには、「配送先」、「宛先」、「送元」が表示される。「配送先」は、配送業者の住所、会社名、営業所名が記載されている。「宛先」は、受取者を識別するための名称であるハンドルネーム（HN）、暗号化された受取者情報、メールアドレスが記載されている。「送元」は、送付者を識別するための名称であるハンドルネーム（HN）、暗号化された送付者情報、メールアドレスが記載されている。このように、ラベルには、受取者の宛先に関する情報及び送付者の個人情報が暗号化されて表示され、送付者

及び受取者の個人情報は一切表示されない。

【 0 0 8 0 】

(3) 受取者暗号情報の復号化

次に、本実施形態にかかる受取者情報の復号化方法を図 2 0 ～図 2 1 に基づいて説明する。なお、図 2 0 は、本実施形態にかかる受取者情報の復号化方法を示す概念図である。図 2 1 は、本実施形態にかかる受取者情報の復号化方法を説明するためのフローチャートである。

【 0 0 8 1 】

まず、ステップ S 4 0 0 で、暗号読取装置（例えばバーコードハンディスキャナ）に配送業者サーバ装置に格納されている秘密鍵 K s を格納する（ステップ S 4 0 0）。

【 0 0 8 2 】

次に、ステップ S 4 0 2 で、配送業者 C は、配送物に添付されたラベルの受取者暗号情報（コードデータ）を、暗号読取装置で読み取る（ステップ S 4 0 2）。

【 0 0 8 3 】

その後、ステップ S 4 0 4 で、図 2 0 に示すように、暗号読取装置は、読み取った受取者暗号情報を、配送業者 C の秘密鍵で復号化して、受取者の宛先情報を取得する（ステップ S 4 0 4）。

【 0 0 8 4 】

さらに、ステップ S 4 0 6 で、図 2 0 に示すように、暗号読取装置の有する印刷機能により受取者の宛先をラベルに印刷する（ステップ S 4 0 6）。

【 0 0 8 5 】

最後に、ステップ S 4 0 8 で、図 2 0 に示すように、印刷したラベルを配送物に貼り付ける（ステップ S 4 0 8）

【 0 0 8 6 】

このようにして、配送業者 C は、受取者 B の宛先を取得して、配送物を配送することができる。

【 0 0 8 7 】

なお、暗号読取装置は、ハンディタイプのプリンタ付きリーダでも良く、自動コンベアに設置して、大量に処理ができるようにしてもよい。なお、固定設置機器の場合には、ネットワークを介して秘密鍵をダウンロードし、さらに、複数の鍵を運用する場合には、鍵の更新などを行なうのが好ましい。また、ハンディタイプの機器の場合には、例えば1日1回の充電の機会を利用して鍵情報の更新を行なうのが有用である。

【0088】

本実施形態においては、公開鍵を使用して、受取者の個人情報（必要に応じて送付者の個人情報）を暗号化するので、個人情報を他人（送付者あるいは受取者）に知られることなく配送物を配送することができる。このとき、受取者の個人情報あるいは送付者の個人情報を格納するためのデータベースが不要となるので、個人情報の流出が最大限防止することができる。さらに、配送業者サーバ装置には、受取者情報を管理するためのデータベースが不要となるので、サーバ管理の手間がなくなるばかりでなく、個人情報を秘密にする配送システムを低コストで実現することができる。さらに、配送業者は、サーバ装置に問い合わせる必要がないので、オフラインで宛名を変換することができる。さらに、ユーザは、自分のID番号を控えておく必要がない。

【0089】

以上、本発明に係る好適な実施の形態について説明したが、本発明はかかる構成に限定されない。当業者であれば、特許請求の範囲に記載された技術思想の範囲内において、各種の修正例及び変更例を想定し得るものであり、それらの修正例及び変更例についても本発明の技術範囲に包含されるものと了解される。

【0090】

例えば、上記実施形態においては、配送業者Cが、受取者情報あるいは送付者情報の暗号化及び復号化サービスを行なっている例を挙げて説明したが、かかるサービスを専門業者が行なうことによっても実施することができる。この場合には、サービス業者を経由して配送業者が配送業務を行うことになる。例えば図22に示すように、受取者Bは、サービス業者Cの公開鍵を使用して受取者情報の暗号化を行い、受取者暗号情報はサービス業者が復号化を行なって配送物にラベ

ルを添付する。また、送付者の身元情報は、サービス業者が暗号化し、送付者の可読情報を張り替る。また、送付者の可読情報は、配送業者に渡される。

【 0 0 9 1 】

また、本実施形態においては、配送サービスは、単独の配送業者でおこなう例を挙げて説明したが、かかる例には限定されない。複数の配送業者で行うことができる。この場合には、図 2 3 に示すように、公開鍵及び秘密鍵の管理及び公開鍵証明書の発行を認証局が行なって、各配送業者に与えることで、暗号化ソフトが共通で使用できると共に、管理の一元化も実現することができる。

【 0 0 9 2 】

また、本実施形態においては、配送業者が 1 つの鍵を有する例を挙げて説明したが、かかる例には限定されない。同じ配送業者が複数の鍵を有することもできる。この場合においても、公開鍵及び秘密鍵の認証局が管理することで実現することができる。例えば秘密鍵が漏洩した場合であっても、認証局が秘密鍵の取り消し手続きをおこなうことができる。また、複数の鍵を用意しておくことで、万一のリスクが分散されることにもなる。この場合には、暗号化配送情報に、暗号化に使用した公開鍵の番号か、証明書を添付することにより、容易に復号化することができる。

【 0 0 9 3 】

また、本実施形態においては、受取者端末装置は、暗号化ファイルを、ネットワークを介して送付者端末装置に送信する例を挙げて説明したが、かかる例には限定されない。ネットワークを介さずに、直接、電子データまたはプリントアウトした結果を送付者に渡すこともできる。

【 0 0 9 4 】

また、本実施形態においては、送付者端末装置は、受取者暗号情報をラベル印刷する例を挙げて説明したがかかる例には限定されない。例えば磁気カード、ICカードなどの各種媒体に格納して配送業者に手渡すこともできる。

【 0 0 9 5 】

また、本実施形態においては、受取者端末装置は、暗号化のための配送業者の公開鍵を配送業者のサイトからダウンロードするように構成した例を挙げて説明

したが、かかる例には限定されない。例えば、公開鍵を予め暗号化プログラムに格納して配布することもできる。

【 0 0 9 6 】

【発明の効果】

公開鍵を使用して、受取者の個人情報（必要に応じて送付者の個人情報）を暗号化するので、個人情報を他人（送付者あるいは受取者）に知られることなく配送物を配送することができる。このとき、受取者の個人情報あるいは送付者の個人情報を格納するためのデータベースが不要となるので、個人情報の流出が最大限防止することができる。さらに、サーバ管理の手間がなくなるばかりでなく、個人情報を秘密にする配送システムを低コストで実現することができる。さらに、配送業者は、サーバ装置に問い合わせる必要がないので、オフラインで宛名を変換することができる。さらに、ユーザは、自分のID番号を控えておく必要がない。また、認証局が鍵を管理するように構成すれば、複数の配送サービス業者が共通のインフラを使用することができる。

【図面の簡単な説明】

【図 1】

第 1 の実施の形態にかかる配送物の配送システムの構成を示すブロック図である。

【図 2】

第 1 の実施の形態にかかる受取者端末装置の構成を示すブロック図である

【図 3】

第 1 の実施の形態にかかる送付者端末装置の構成を示すブロック図である

【図 4】

第 1 の実施の形態にかかる配送業者サーバ装置の構成を示すブロック図である。

【図 5】

第 1 の実施の形態にかかる配送物の配送方法を示す概念図である。

【図 6】

第 1 の実施の形態にかかる配送物の配送方法を示すフローチャートである。

【図 7】

第 1 の実施の形態にかかる送付者情報を暗号化する場合の配送物の配送方法を示す概念図である。

【図 8】

第 1 の実施の形態にかかる第 1 の暗号方法を示す概念図である。

【図 9】

第 1 の実施の形態にかかる第 1 の暗号方法を示すフローチャートである。

【図 1 0】

第 1 の暗号化方法におけるコンピュータ画面表示を示す説明図である。

【図 1 1】

第 1 の暗号化方法におけるコンピュータ画面表示を示す説明図である。

【図 1 2】

第 1 の暗号化方法におけるコンピュータ画面表示を示す説明図である。

【図 1 3】

第 2 実施の形態にかかる第 1 の暗号方法を示す概念図である。

【図 1 4】

第 2 の実施の形態にかかる第 1 の暗号方法を示すフローチャートである。

【図 1 5】

第 2 の暗号化方法におけるコンピュータ画面表示を示す説明図である。

【図 1 6】

第 2 の暗号化方法におけるコンピュータ画面表示を示す説明図である。

【図 1 7】

第 2 の暗号化方法におけるコンピュータ画面表示を示す説明図である。

【図 1 8】

受取者暗号情報をラベルに表示した一例を示す説明図である。

【図 1 9】

受取者暗号情報及び送付者暗号情報をラベルに表示した一例を示す説明図である。

【図 2 0】

第 1 の実施の形態にかかる受取者情報の復号化方法を示す概念図である。

【図 2 1】

第 1 の実施の形態にかかる受取者情報の復号化方法を説明するためのフローチャートである。

【図 2 2】

サービス業者を経由して配送業者が配送業務を行う場合の配送システムを示す概念図である。

【図 2 3】

複数の配送業者が配送業務を行う場合の配送システムを示す概念図である。

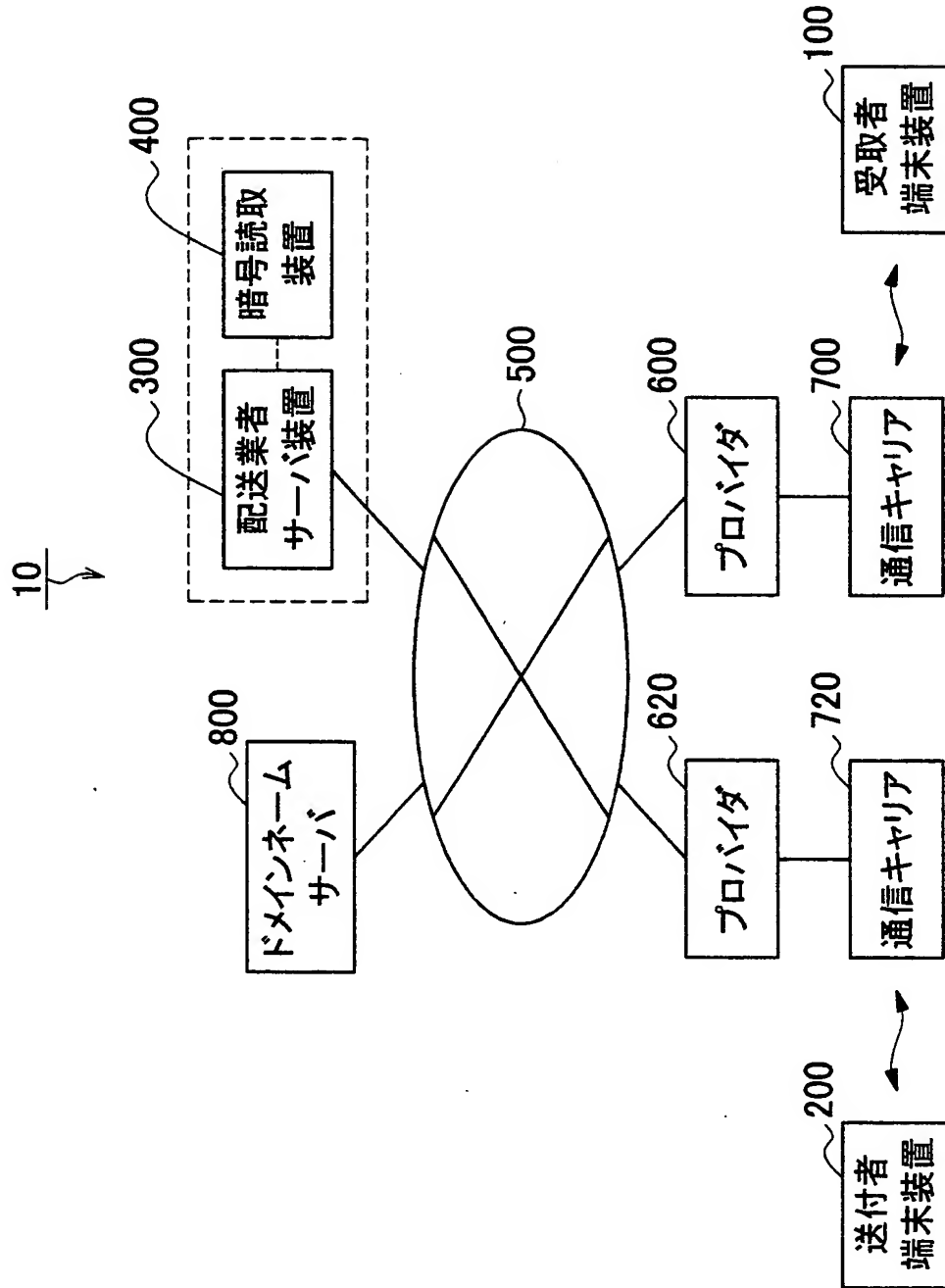
【符号の説明】

- 1 0 配送システム
- 1 0 0 受取者端末装置
- 2 0 0 送付者端末装置
- 3 0 0 配送業者サーバ装置
- 3 1 0 C P U
- 3 2 0 通信ユニット
- 3 3 0 メモリ
- 3 4 0 暗号プログラム管理手段
- 3 5 0 公開鍵管理手段
- 3 6 0 秘密鍵管理手段
- 3 7 0 コンテンツデータベース
- 4 0 0 暗号読取装置
- 5 0 0 ネットワーク
- 6 0 0, 6 2 0 プロバイタ
- 7 0 0, 7 2 0 通信キャリア
- 8 0 0 ドメインネームサーバ

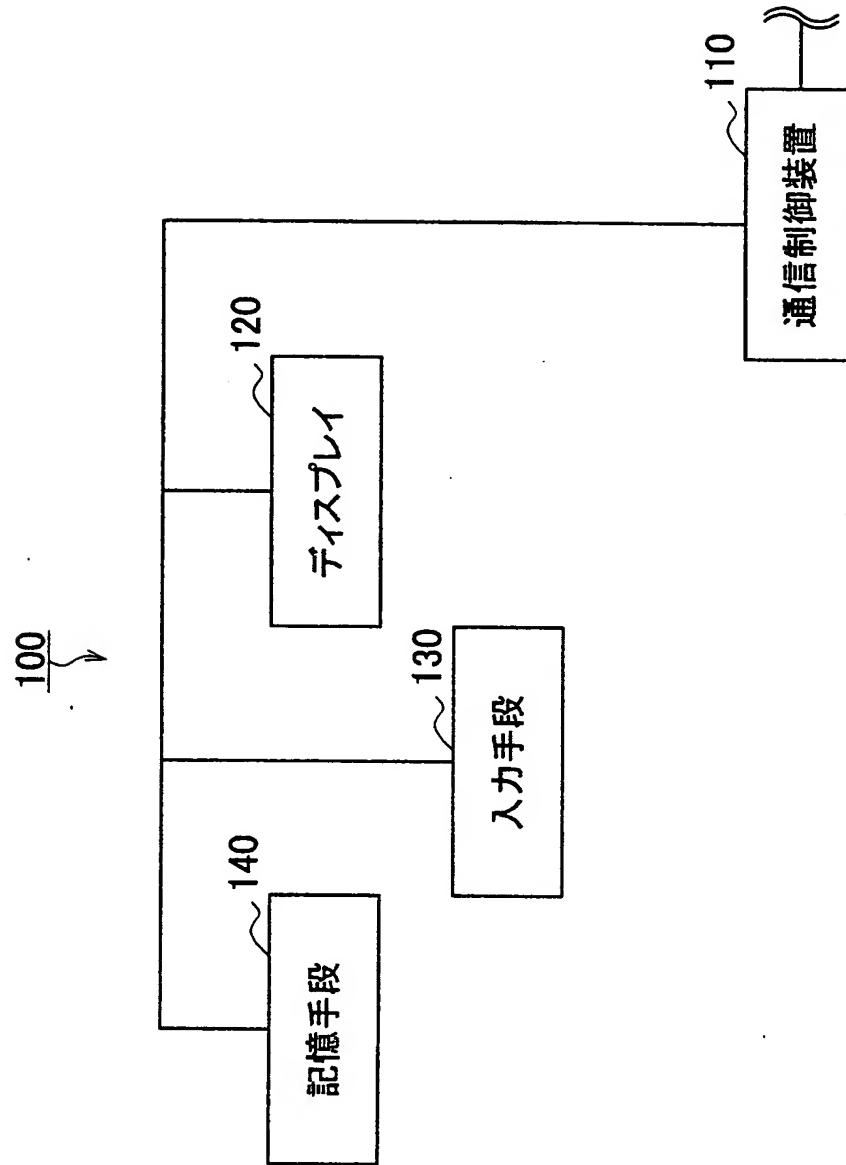
【書類名】

図面

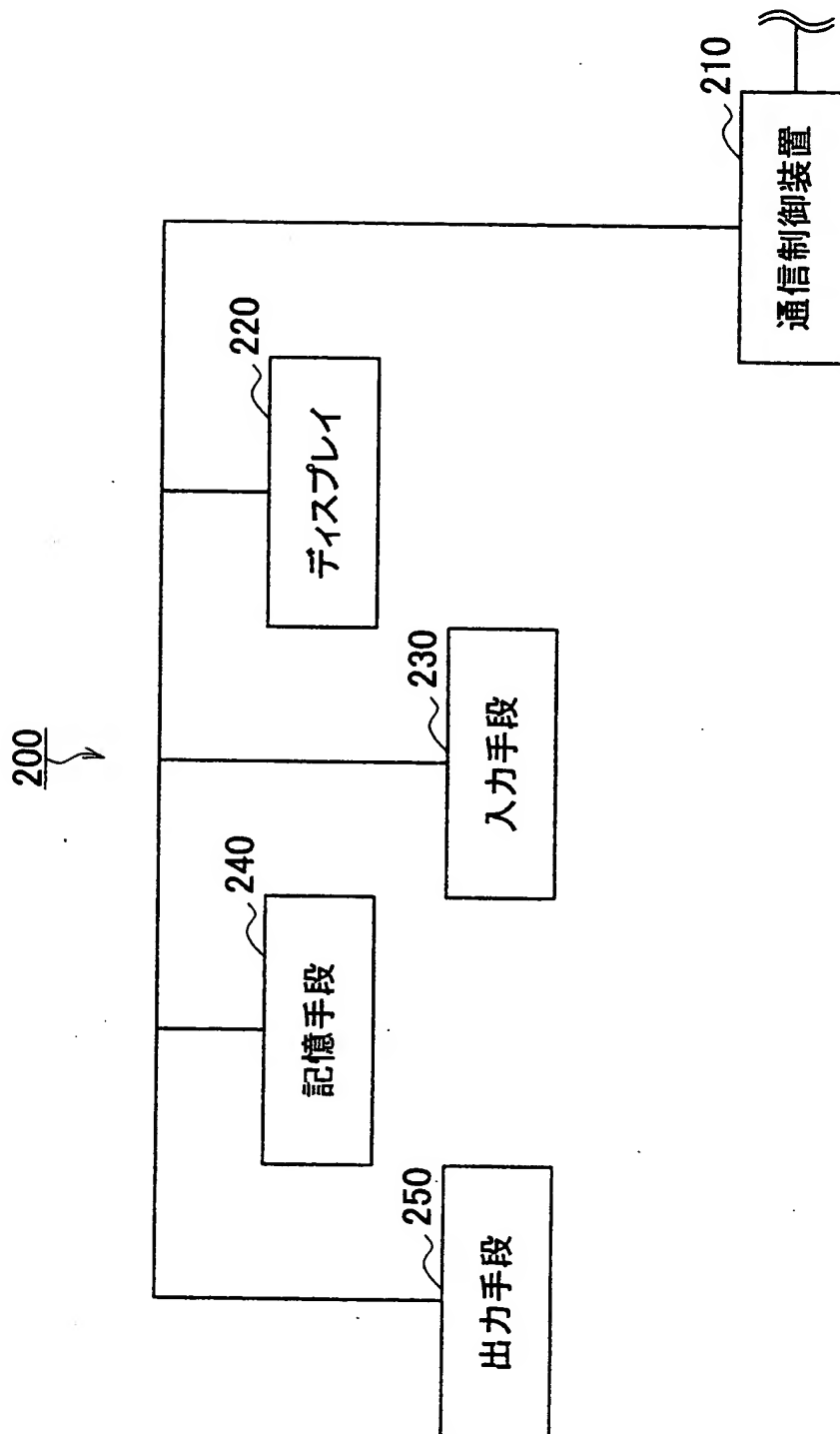
【図 1】



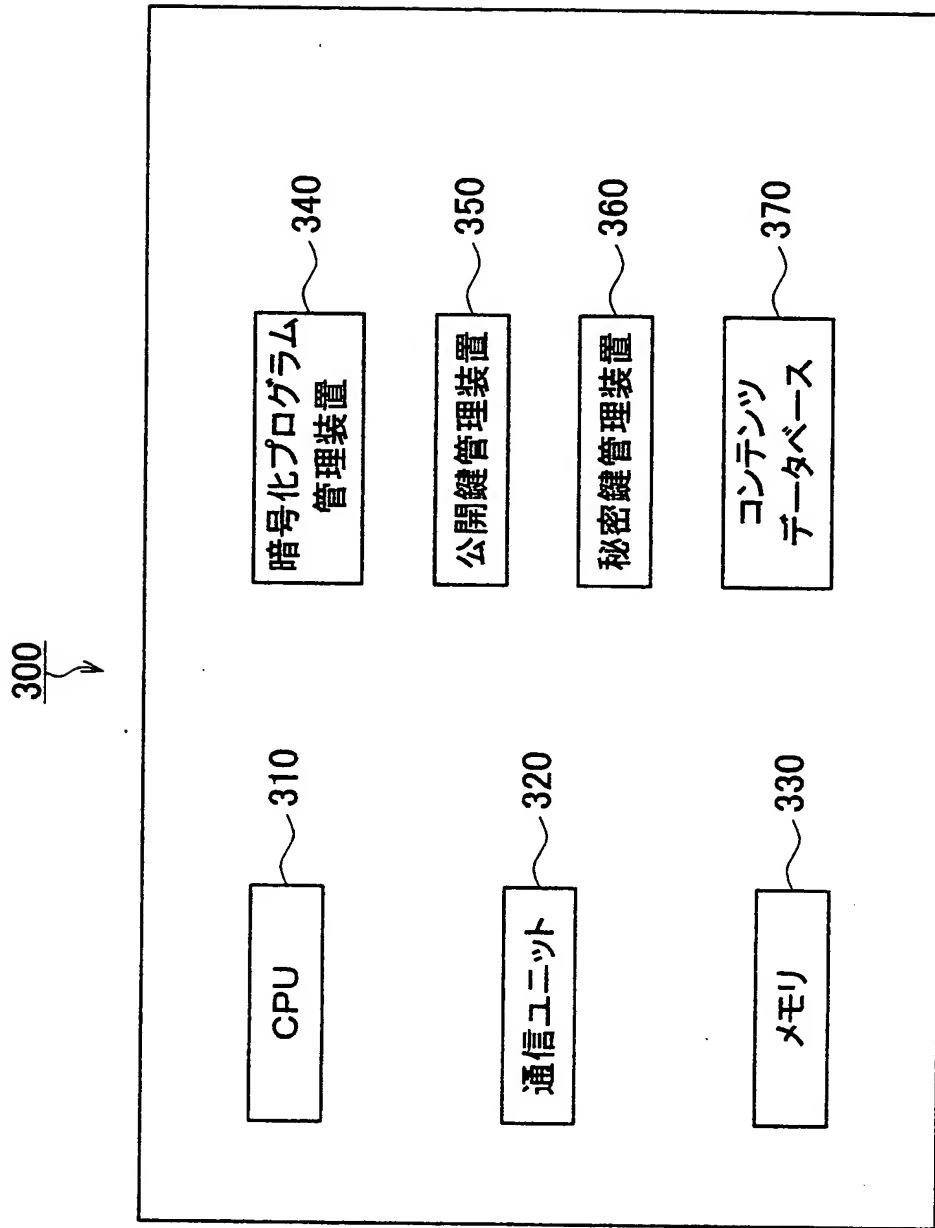
【図 2】



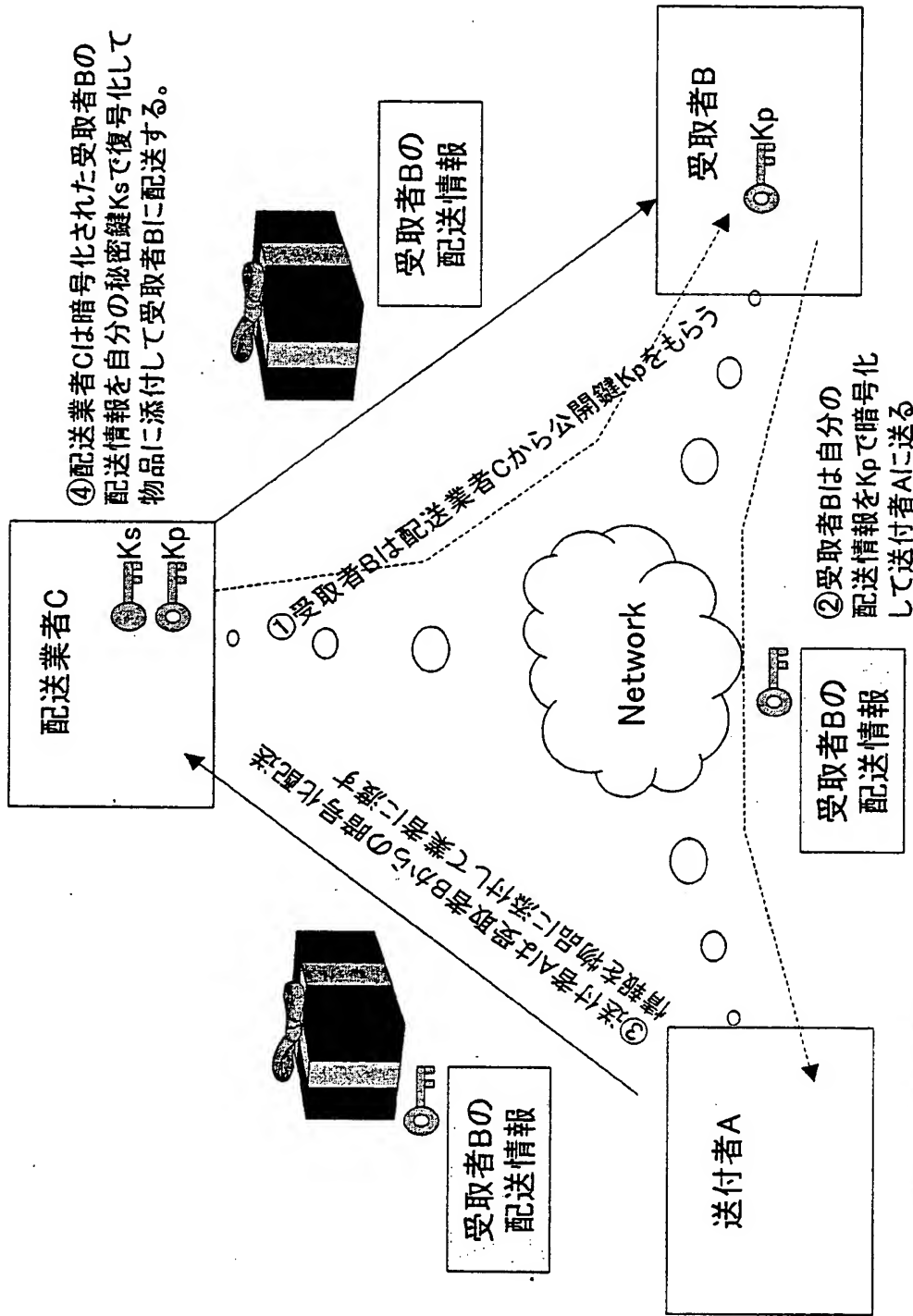
【図 3】



【図 4】

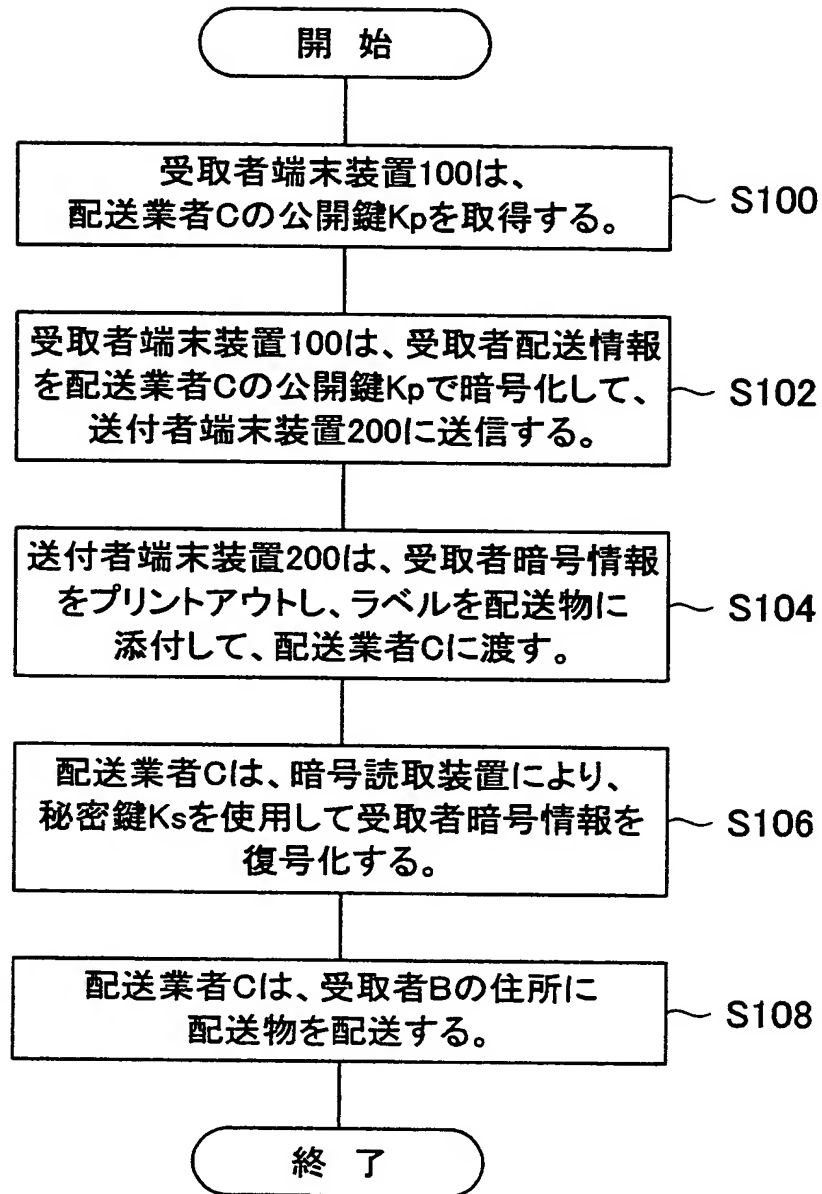


【図 5】

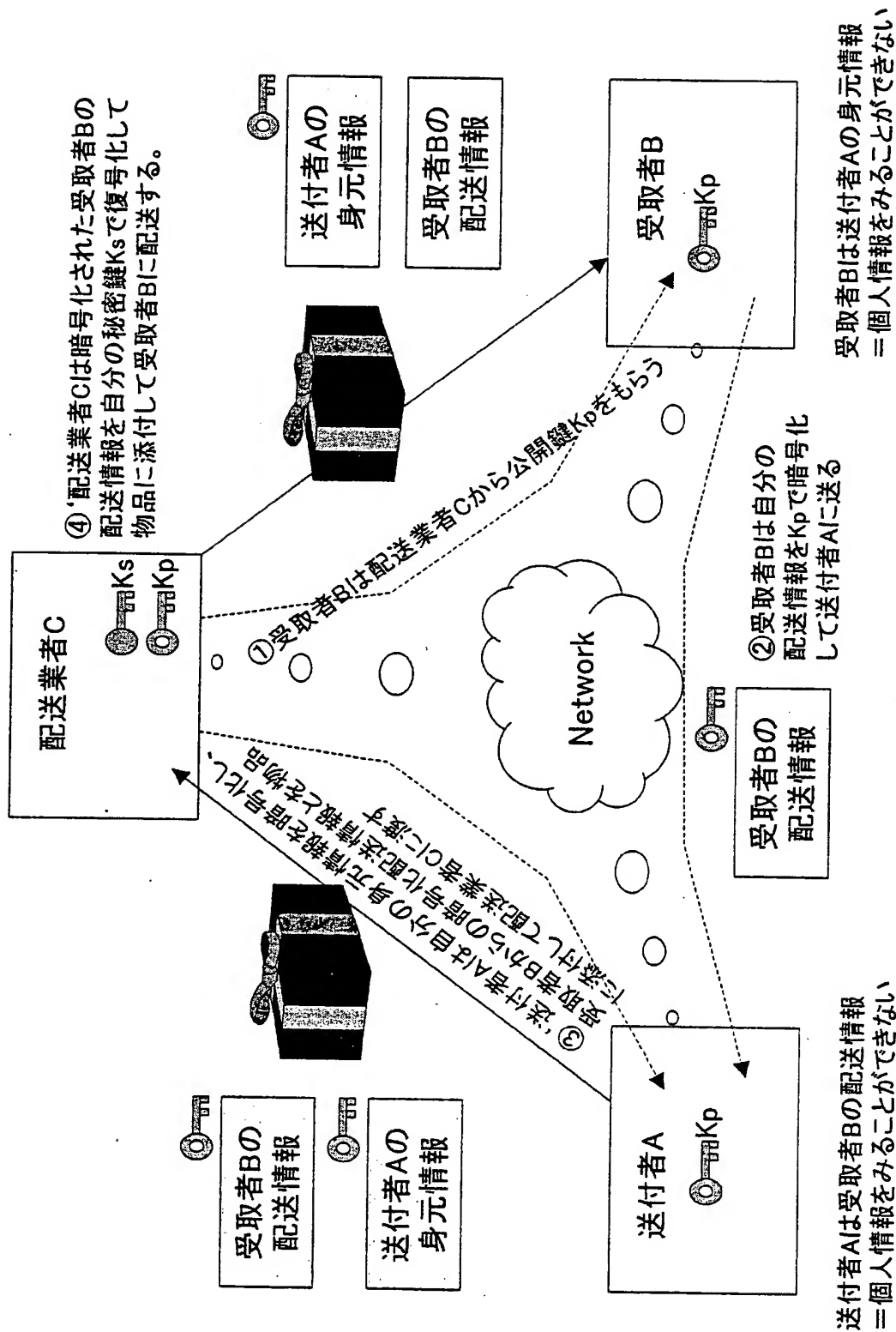


送付者Aは受取者Bの配送情報
＝個人情報を見ることができない

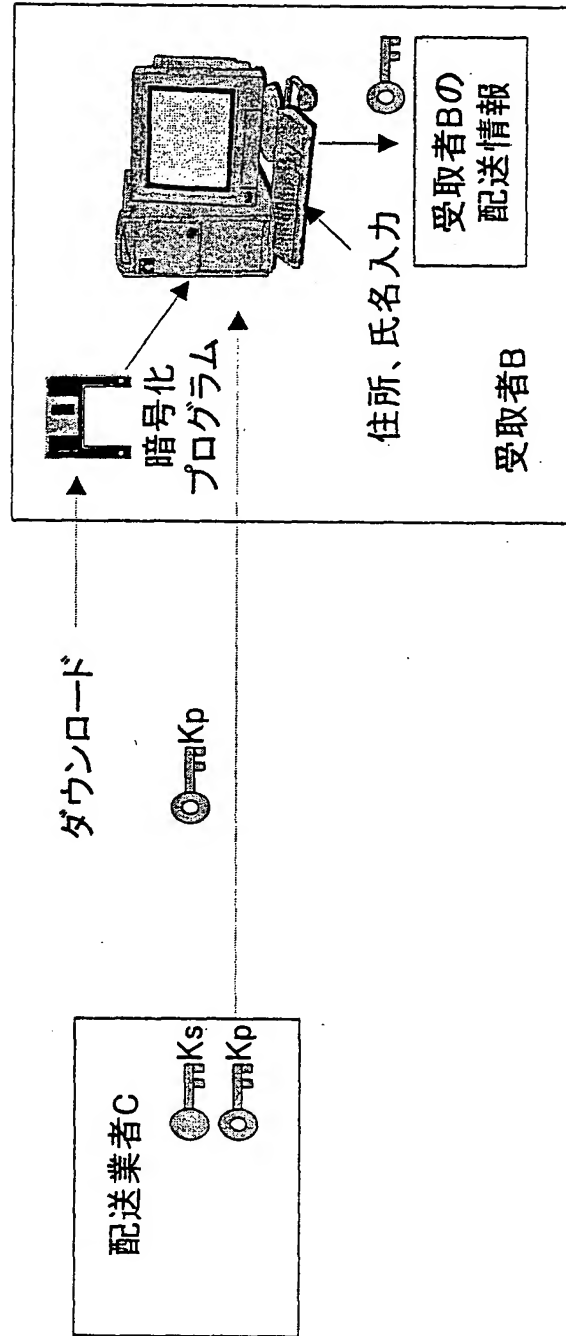
【図 6】



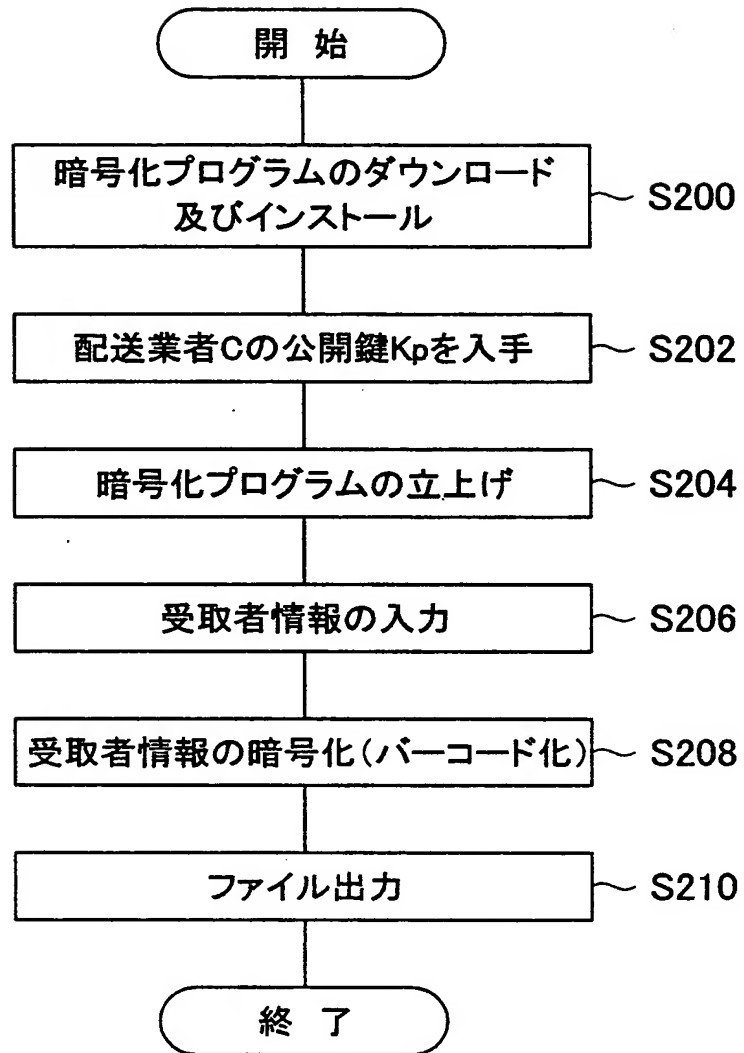
【図 7】



【図8】



【図 9】



【図 1 0】

住所・氏名を入力して下さい

ハンドルネーム

〒

住 所

氏 名

TEL

【図 1 1】

宛先は

〒〇〇〇—〇〇〇〇

東京都〇〇区△△-----

〇〇〇〇様

TEL 03-XXXX-----

よろしいですか？

【図 1 2】

○ 暗号化が完了しました

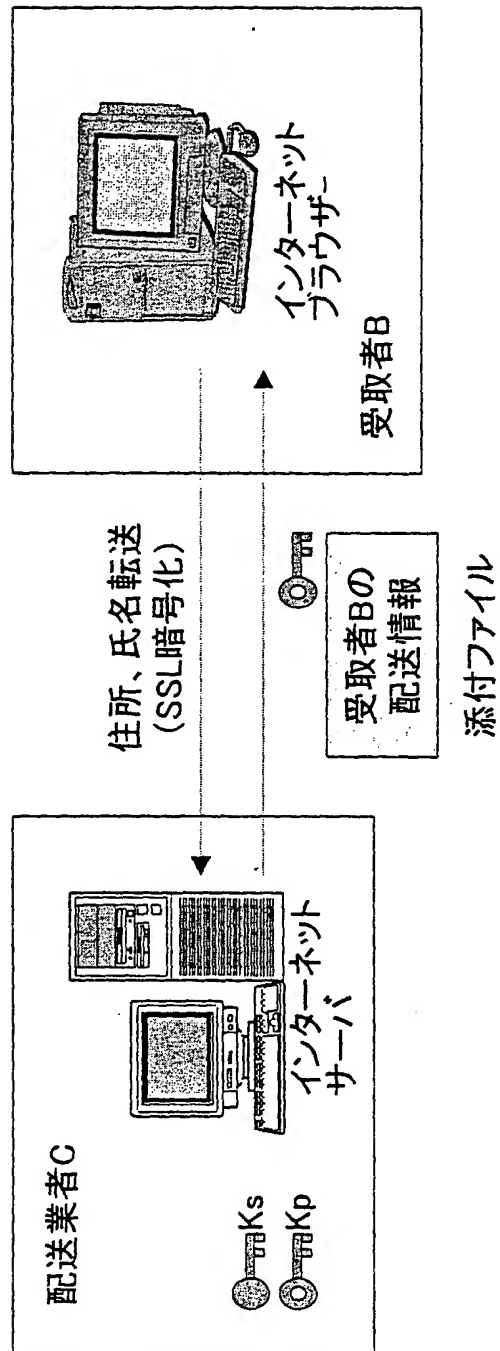
○ 保存するディレクトリを指定して下さい

C:-----¥-----

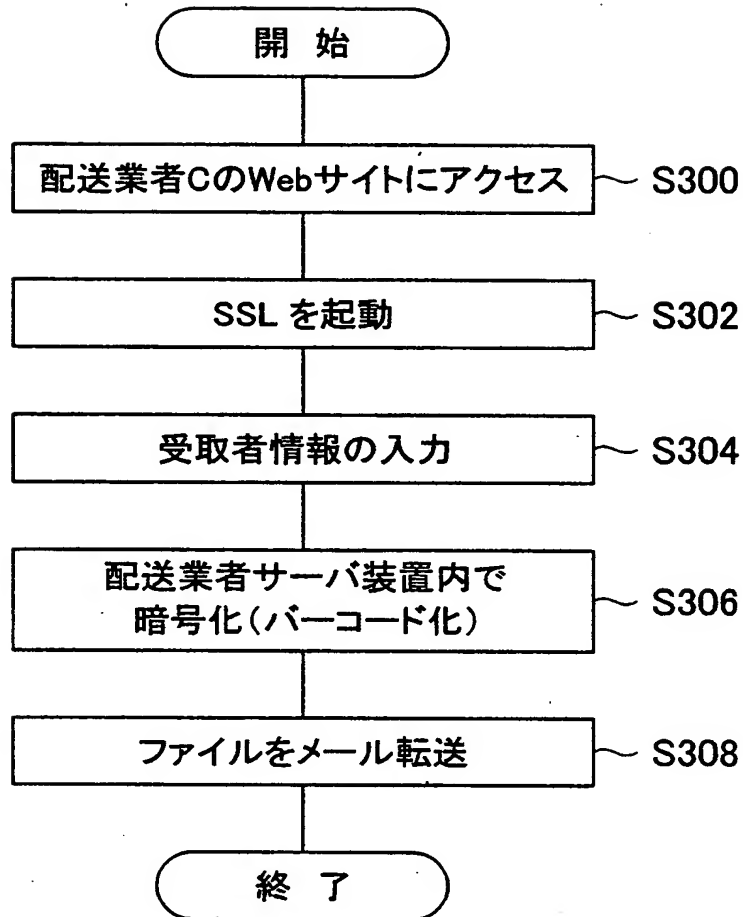
参 照

OK

【図13】



【図 14】



【図 15】

住所・氏名を入力して下さい

ハンドルネーム	<input style="width: 90%;" type="text"/>
〒	<input style="width: 45%;" type="text"/> <input style="width: 5%; text-align: center; border: 1px solid black;" type="button" value="▽"/>
住 所	<input style="width: 90%;" type="text"/>
氏 名	<input style="width: 90%;" type="text"/>
TEL	<input style="width: 90%;" type="text"/>

【図16】

宛先は
〒〇〇〇—〇〇〇〇
東京都〇〇区△△-----
〇〇〇〇様
TEL 03-XXXX-----
よろしいですか？

OK
(暗号化)

【図17】

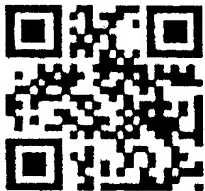
○ メールアドレスに
暗号化ファイルを送信します

-----@-----ne.jp 参照

OK

【図 1 8】

配送先	〇〇区〇〇町〇〇-〇〇 〇〇運送株式会社 五反田営業所
宛先	HN: ナナッチ



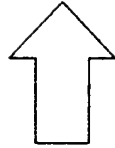
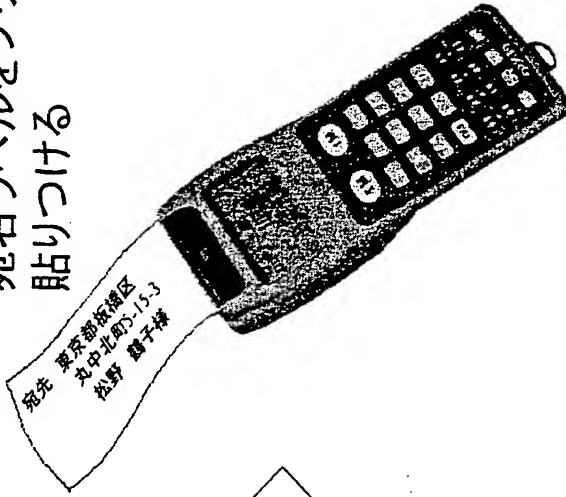
mail: nana-chi@xb3.so-net.ne.jp

【図 19】

配送先	〇〇区〇〇町〇〇-〇〇 〇〇運送株式会社 五反田営業所
宛先	HN: ナナッチ  mail: nana-chi@xb3.so-net.ne.jp
送元	HN: ハムどん  mail: ham-don@excite.co.jp

【図20】

宛名ラベルをプリントし
貼りつける



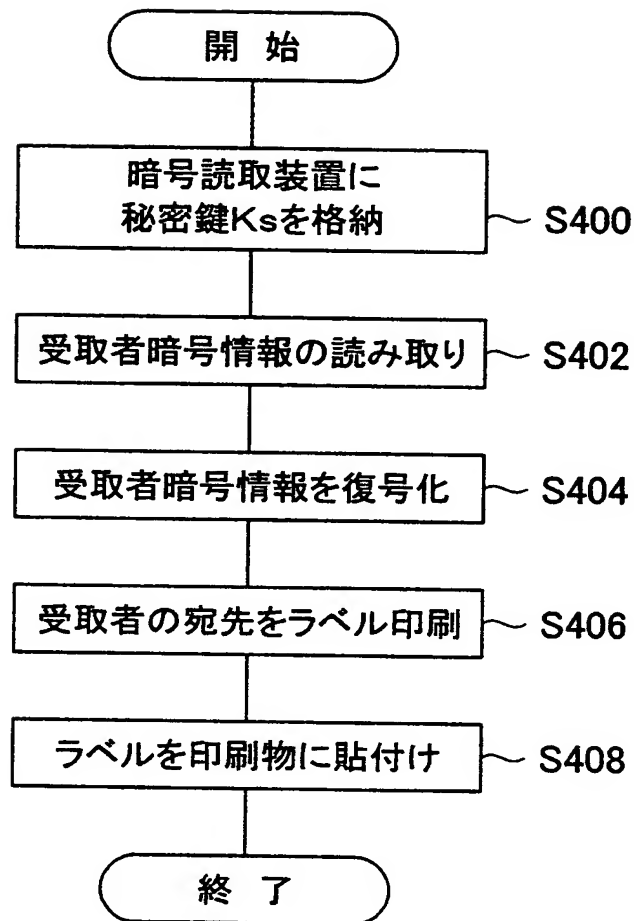
バーコードをハンディスキャナで
読み取る

受取者が物品を受け取る
ときのラベル表示例

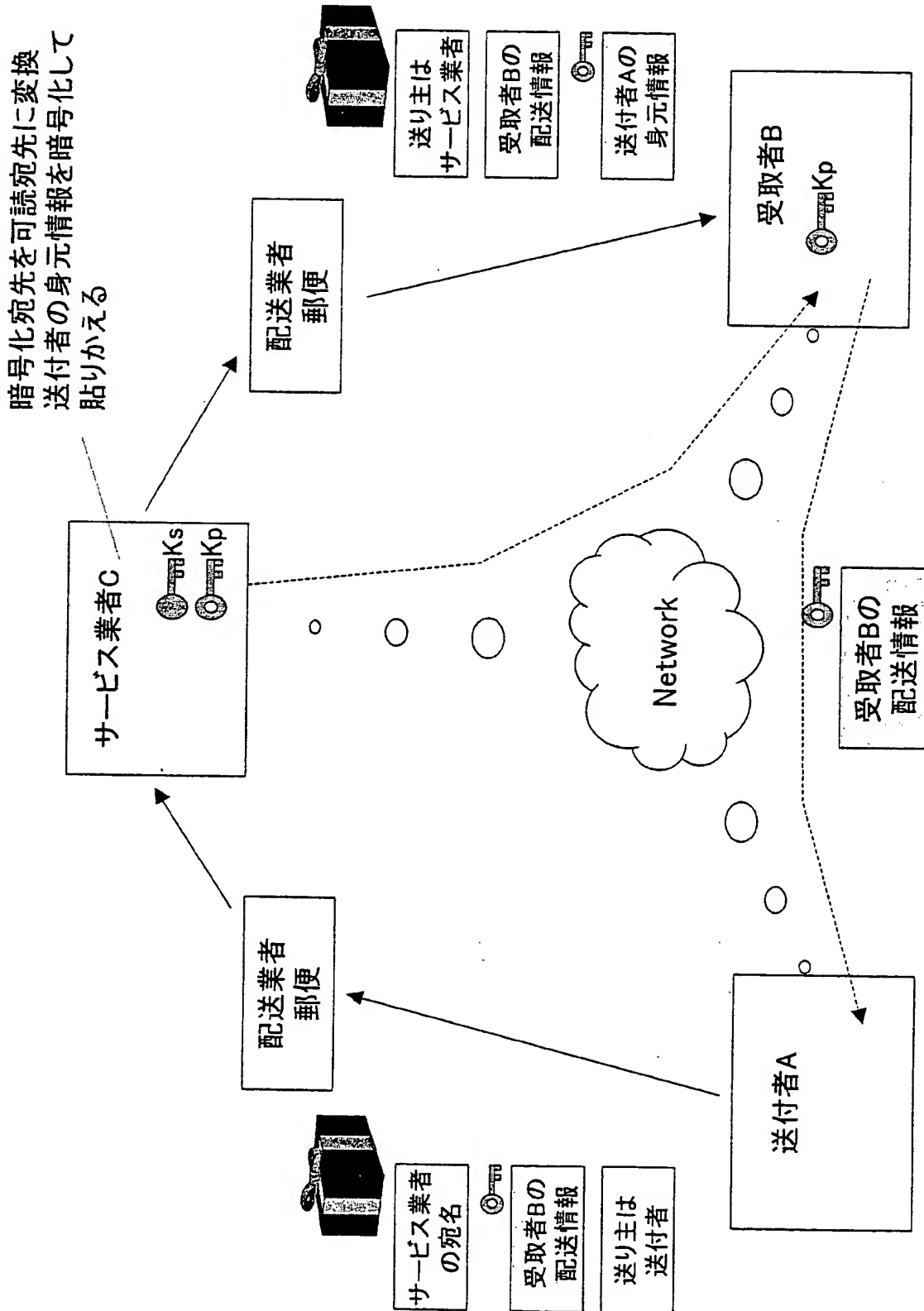
宛先	東京都板橋区 丸中北町5-15-3 松野 鶴子 様
送元	HN: ハムどん mail: ham-don@excite.co.jp



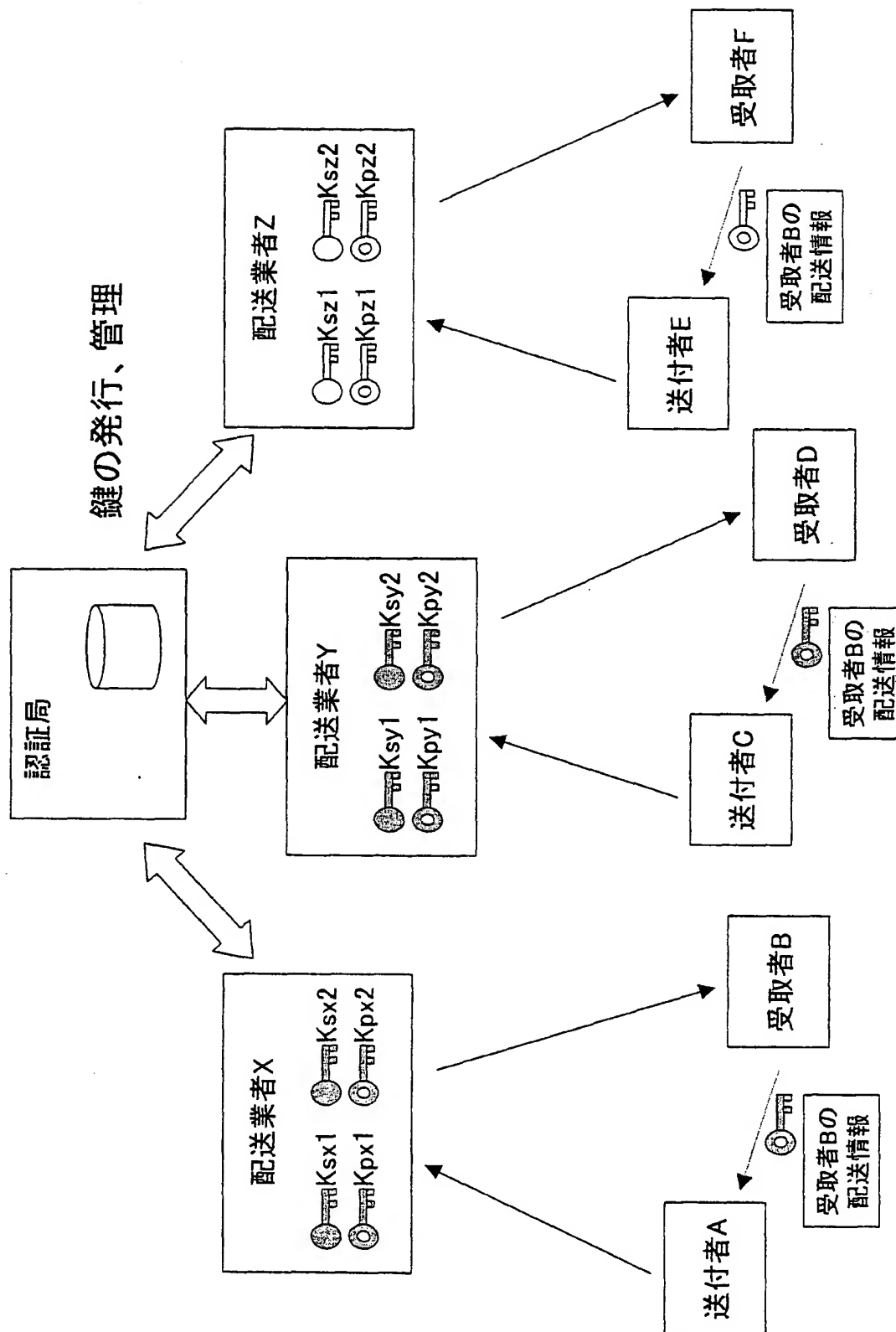
【図 2 1】



【図 22】



【図 23】



【書類名】 要約書

【要約】

【課題】 厳密な管理が必要な情報を格納するデータベースを設置することなく、送付者及び受取人の個人情報を秘密にした状態で配送物を配送する。

【解決手段】 受取者端末装置は、配送業者サーバ装置から配送業者の公開鍵を取得し、公開鍵を使用して、少なくとも配送物の配送に必要な受取者の個人情報からなる受取者情報を予めダウンロードした前記配送業者の暗号化プログラムにより暗号化し、受取者暗号情報を送付者端末装置に送信し、送付者端末装置は、送信された受取者暗号情報を配送業者に委託する配送物に添付するために出力し、出力された受取者暗号情報は、配送業者の有する暗号読取装置により、配送業者の秘密鍵を使用して受取者暗号情報を復号化されて、受取人の配達先の情報が配送業者に取得される。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社
2. 変更年月日 2003年 5月15日
[変更理由] 名称変更
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社